Publ. Math. Debrecen
79/3-4 (2011), 687–697
DOI: 10.5486/PMD.2011.5106

On the counting function of sets with even partition functions

By FETHI BEN SAÏD (Monastir) and JEAN-LOUIS NICOLAS (Villeurbanne)

To Kálmán Győry, Attila Pethő, János Pintz and András Sárközy
for their nice works in number theory

Abstract. Let q be an odd positive integer and $P \in \mathbb{F}_2[z]$ be of order q and such that $P(0) = 1$. We denote by $\mathcal{A} = \mathcal{A}(P)$ the unique set of positive integers satisfying $\sum_{n=0}^{\infty} p(\mathcal{A}, n) z^n \equiv P(z) \pmod{2}$, where $p(\mathcal{A}, n)$ is the number of partitions of n with parts in $\mathcal{A}$. In [5], it is proved that if $\mathcal{A}(P, x)$ is the counting function of the set $\mathcal{A}(P)$ then $\mathcal{A}(P, x) \ll x(\log x)^{-r/\varphi(q)}$, where r is the order of 2 modulo q and φ is the Euler's function. In this paper, we improve on the constant $c = c(q)$ for which $\mathcal{A}(P, x) \ll x(\log x)^{-c}$.

1. Introduction

Let $\mathbb{N}$ be the set of positive integers and $\mathcal{A} = \{a_1, a_2, \dots\}$ be a subset of $\mathbb{N}$. For $n \in \mathbb{N}$, we denote by $p(\mathcal{A}, n)$ the number of partitions of n with parts in $\mathcal{A}$, i.e. the number of solutions of the equation

$$a_1 x_1 + a_2 x_2 + \cdots = n,$$

in non-negative integers $x_1, x_2, \dots$. We set $p(\mathcal{A}, 0) = 1$.

Let $\mathbb{F}_2$ be the field with two elements and $f = 1 + \epsilon_1 z + \cdots + \epsilon_N z^N + \cdots \in \mathbb{F}_2[[z]]$. NICOLAS et al. proved (see [13], [4] and [11]) that there is a unique subset

Mathematics Subject Classification: 11P83.
Key words and phrases: sets with even partition functions, bad and semi-bad primes, order of a polynomial, Selberg–Delange formula.

$\mathcal{A} = \mathcal{A}(f)$ of $\mathbb{N}$ such that

$$\sum_{n=0}^{\infty} p(\mathcal{A}, n) z^n \equiv f(z) \pmod{2}. \tag{1.1}$$

When f is a rational fraction, it has been shown in [11] that there is a polynomial U such that $\mathcal{A}(f)$ can be easily determined from $\mathcal{A}(U)$. When f is a general power series, nothing about the behaviour of $\mathcal{A}(f)$ is known. From now on, we shall restrict ourselves to the case $f = P$, where

$$P = 1 + \epsilon_1 z + \cdots + \epsilon_N z^N \in \mathbb{F}_2[z]$$

is a polynomial of degree $N \geq 1$.

Let $A(P, x)$ be the counting function of the set $\mathcal{A}(P)$, i.e.

$$A(P, x) = |\{n : 1 \leq n \leq x,\ n \in \mathcal{A}(P)\}|. \tag{1.2}$$

In [10], it is proved that

$$A(P, x) \geq \frac{\log x}{\log 2} - \frac{\log(N+1)}{\log 2}. \tag{1.3}$$

More attention was paid on upper bounds for $A(P, x)$. In [5, Theorem 3], it was observed that when P is a product of cyclotomic polynomials, the set $\mathcal{A}(P)$ is a union of geometric progressions of quotient 2 and so $A(P, x) = \mathcal{O}(\log x)$.

Let the decomposition of P into irreducible factors over $\mathbb{F}_2[z]$ be

$$P = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_l^{\alpha_l}.$$

We denote by β_i, $1 \leq i \leq l$, the order of $P_i(z)$, that is the smallest positive integer such that $P_i(z)$ divides $1 + z^{\beta_i}$ in $\mathbb{F}_2[z]$; it is known that β_i is odd (cf. [12]). We set

$$q = q(P) = \operatorname{lcm}(\beta_1, \beta_2, \ldots, \beta_l). \tag{1.4}$$

If $q = 1$ then $P(z) = 1 + z$ and $\mathcal{A}(P) = \{2^k,\ k \geq 0\}$, so that $A(P, x) = \mathcal{O}(\log x)$. We may suppose that $q \geq 3$. Now, let

$$\sigma(\mathcal{A}, n) = \sum_{d|n,\ d \in \mathcal{A}} d = \sum_{d|n} d\chi(\mathcal{A}, d), \tag{1.5}$$

where $\chi(\mathcal{A}, .)$ is the characteristic function of the set $\mathcal{A}$,

$$\chi(\mathcal{A}, d) = \begin{cases} 1 & \text{if } d \in \mathcal{A} \\ 0 & \text{otherwise.} \end{cases}$$

In [6] (see also [3] and [2]), it is proved that for all $k \geq 0$, q is a period of the sequence $(\sigma(\mathcal{A}, 2^k n) \mod 2^{k+1})_{n \geq 1}$, i.e.

$$n_1 \equiv n_2 \pmod{q} \Rightarrow \sigma(\mathcal{A}, 2^k n_1) \equiv \sigma(\mathcal{A}, 2^k n_2) \pmod{2^{k+1}} \tag{1.6}$$

and q is the smallest integer such that (1.6) holds for all $k's$. Moreover, if n_1 and n_2 satisfy $n_2 \equiv 2^a n_1 \pmod{q}$ for some $a \geq 0$, then

$$\sigma(\mathcal{A}, 2^k n_2) \equiv \sigma(\mathcal{A}, 2^k n_1) \pmod{2^{k+1}}. \tag{1.7}$$

If m is odd and $k \geq 0$, let

$$S_{\mathcal{A}}(m, k) = \chi(\mathcal{A}, m) + 2\chi(\mathcal{A}, 2m) + \ldots + 2^k \chi(\mathcal{A}, 2^k m). \tag{1.8}$$

It follows that for $n = 2^k m$, one has

$$\sigma(\mathcal{A}, n) = \sigma(\mathcal{A}, 2^k m) = \sum_{d|m} d S_{\mathcal{A}}(d, k), \tag{1.9}$$

which, by Möbius inversion formula, gives

$$m S_{\mathcal{A}}(m, k) = \sum_{d|m} \mu(d) \sigma\left(\mathcal{A}, \frac{n}{d}\right) = \sum_{d|\overline{m}} \mu(d) \sigma\left(\mathcal{A}, \frac{n}{d}\right), \tag{1.10}$$

where μ is the Möbius's function and $\overline{m} = \prod_{p|m} p$ is the radical of m, with $\overline{1} = 1$.

In [7] and [9], precise descriptions of the sets $\mathcal{A}(1+z+z^3)$ and $\mathcal{A}(1+z+z^3+z^4+z^5)$ are given and asymptotics to the related counting functions are obtained,

$$A(1+z+z^3, x) \sim c_1 \frac{x}{(\log x)^{\frac{3}{4}}}, \qquad x \to \infty, \tag{1.11}$$

$$A(1+z+z^3+z^4+z^5, x) \sim c_2 \frac{x}{(\log x)^{\frac{1}{4}}}, \qquad x \to \infty, \tag{1.12}$$

where $c_1 = 0.937\ldots$, $c_2 = 1.496\ldots$. In [1], the sets $\mathcal{A}(P)$ are considered when P is irreducible of prime order q and such that the order of 2 in $(\mathbb{Z}/q\mathbb{Z})^*$ is $\frac{q-1}{2}$. This situation is similar to that of $\mathcal{A}(1+z+z^3)$, and formula (1.11) can be extended to $A(P, x) \sim c' x (\log x)^{-3/4}$, $x \to \infty$, for some constant c' depending on P.

Let $P = QR$ be the product of two coprime polynomials in $\mathbb{F}_2[z]$. In [4], the following is given

$$A(P, x) \leq A(Q, x) + A(R, x) \tag{1.13}$$

and

$$|A(P, x) - A(R, x)| \leq \sum_{0 \leq i \leq \frac{\log x}{\log 2}} A\left(Q, \frac{x}{2^i}\right). \tag{1.14}$$

As an application of (1.14), choosing $Q = 1 + z + z^3$, $R = 1 + z + z^3 + z^4 + z^5$ and $P = QR$, we get from (1.11)–(1.14),

$$A(P,x) \sim A(R,x) \sim c_2 x (\log x)^{-1/4}, \quad x \to \infty.$$

In [5], a claim of NICOLAS and SÁRKÖZY [15], that some polynomials with $A(P,x) \asymp x$ may exist, was disapproved. More precisely, the following was obtained

Theorem 1.1. *Let $P \in \mathbb{F}_2[z]$ be such that $P(0) = 1$, $\mathcal{A} = \mathcal{A}(P)$ be the unique set obtained from (1.1) and q be the odd number defined by (1.4). Let r be the order of 2 modulo q, that is the smallest positive integer such that $2^r \equiv 1 \pmod{q}$. We shall say that a prime $p \neq 2$ is a bad prime if*

$$\exists\, i, \quad 0 \le i \le r-1 \text{ and } p \equiv 2^i \pmod{q}. \tag{1.15}$$

(i) *If p is a bad prime, we have $\gcd(p,n) = 1$ for all $n \in \mathcal{A}$.*

(ii) *There exists an absolute constant c_3 such that for all $x > 1$,*

$$A(P,x) \le 7(c_3)^r \frac{x}{(\log x)^{\frac{r}{\varphi(q)}}}, \tag{1.16}$$

where φ is Euler's function.

2. The sets of bad and semi-bad primes

Let q be an odd integer ≥ 3 and r be the order of 2 modulo q. Let us call "bad classes" the elements of

$$\mathcal{E}(q) = \{1, 2, \ldots, 2^{r-1}\} \subset (\mathbb{Z}/q\mathbb{Z})^*. \tag{2.1}$$

From (1.15), we know that an odd prime p is bad if $p \mod q$ belongs to $\mathcal{E}(q)$. The set of bad primes will be denoted by $\mathcal{B}$. The fact that no element of $\mathcal{A}(P)$ is divisible by a bad prime (cf. Theorem 1.1 (i)) has given (cf. [5]) the upper bound (1.16). Two other sets of primes will be used to improve (1.16) cf. Theorem 2.1 below.

Remark 2.1. 2 is not a bad prime although it is a bad class.

Definition 2.1. A class of $(\mathbb{Z}/q\mathbb{Z})^*$ is said semi-bad if it does not belong to $\mathcal{E}(q)$ and its square does. A prime p is called semi-bad if its class modulo q is semi-bad. We denote by $\mathcal{E}'(q)$ the set of semi-bad classes, so that

$$p \text{ semi-bad} \iff p \mod q \in \mathcal{E}'(q).$$

We denote by $|\mathcal{E}'(q)|$ the number of elements of $\mathcal{E}'(q)$.

Lemma 2.1. *Let q be an odd integer ≥ 3, r be the order of 2 modulo q and*

$$q_2 = \begin{cases} 1 & \text{if 2 is a square modulo } q \\ 0 & \text{if not.} \end{cases}$$

The number $|\mathcal{E}'(q)|$ of semi-bad classes modulo q is given by

$$\begin{aligned} |\mathcal{E}'(q)| &= 2^{\omega(q)}\left(\left\lfloor\frac{r+1}{2}\right\rfloor + q_2\left\lfloor\frac{r}{2}\right\rfloor\right) - r \\ &= \begin{cases} r(2^{\omega(q)-1}-1) & \text{if } r \text{ is even and } q_2 = 0 \\ r(2^{\omega(q)}-1) & \text{otherwise,} \end{cases} \end{aligned} \tag{2.2}$$

where $\omega(q)$ is the number of distinct prime factors of q and $\lfloor x \rfloor$ is the floor of x.

Proof. We have to count the number of solutions of the r congruences

$$E_i : x^2 \equiv 2^i \pmod{q}, \quad 0 \leq i \leq r-1,$$

which do not belong to $\mathcal{E}(q)$. The number of solutions of E_0 is $2^{\omega(q)}$. The contribution of E_i when i is even is equal to that of E_0 by the change of variables $x = 2^{i/2}\xi$, so that the total number of solutions, in $(\mathbb{Z}/q\mathbb{Z})^*$, of the E_i's for i even is equal to $\lfloor\frac{r+1}{2}\rfloor 2^{\omega(q)}$.

The number of odd $i's$, $0 \leq i \leq r-1$, is equal to $\lfloor\frac{r}{2}\rfloor$. The contribution of all the E_i's for these $i's$ are equal and vanish if $q_2 = 0$. When $q_2 = 1$, E_1 has $2^{\omega(q)}$ solutions in $(\mathbb{Z}/q\mathbb{Z})^*$. Hence the total number of solutions, in $(\mathbb{Z}/q\mathbb{Z})^*$, of the E_i's for i odd is equal to $q_2\lfloor\frac{r}{2}\rfloor 2^{\omega(q)}$.

Now, we have to remove those solutions which are in $\mathcal{E}(q)$. But any element 2^i, $0 \leq i \leq r-1$, from $\mathcal{E}(q)$ is a solution of the congruence $x^2 \equiv 2^j \pmod{q}$, where $j = 2i \mod r$. Hence

$$|\mathcal{E}'(q)| = 2^{\omega(q)}\left(\left\lfloor\frac{r+1}{2}\right\rfloor + q_2\left\lfloor\frac{r}{2}\right\rfloor\right) - r.$$

The second formula in (2.2) follows by noting that $q_2 = 1$ when r is odd. □

Definition 2.2. A set of semi-bad classes is called a coherent set if it is not empty and if the product of any two of its elements is a bad class.

Lemma 2.2. *Let b be a semi-bad class; then*

$$\mathcal{C}_b = \{b, 2b, \ldots, 2^{r-1}b\}$$

is a coherent set. There are no coherent sets with more than r elements.

PROOF. First, we observe that, for $0 \le u \le r-1$, $2^u b$ is semi-bad and, for $0 \le u < v \le r-1$, $(2^u b)(2^v b)$ is bad so that $\mathcal{C}_b$ is coherent.

Further, let $\mathcal{F}$ be a set of semi-bad classes with more than r elements; there exists in $\mathcal{F}$ two semi-bad classes a and b such that $a \notin \mathcal{C}_b$. Let us prove that ab is not bad. Indeed, if $ab \equiv 2^u \pmod{q}$ for some u, we would have $a \equiv 2^u b^{-1} \pmod{q}$. But, as b is semi-bad, b^2 is bad, i.e. $b^2 \equiv 2^v \pmod{q}$ for some v, which would imply $b \equiv 2^v b^{-1} \pmod{q}$, $b^{-1} \equiv b2^{-v} \pmod{q}$, $a \equiv 2^{u-v} b \pmod{q}$ and $a \in \mathcal{C}_b$, a contradiction. Therefore, $\mathcal{F}$ is not coherent. □

Lemma 2.3. *If $\omega(q) = 1$ and $\varphi(q)/r$ is odd, then $\mathcal{E}'(q) = \emptyset$; while if $\varphi(q)/r$ is even, the set of semi-bad classes $\mathcal{E}'(q)$ is a coherent set of r elements.*

If $\omega(q) \ge 2$, then $\mathcal{E}'(q) \neq \emptyset$ and there exists a coherent set C with $|C| = r$.

PROOF. If $\omega(q) = 1$, q is a power of a prime number and the group $(\mathbb{Z}/q\mathbb{Z})^*$ is cyclic. Let g be some generator and d be the smallest positive integer such that $g^d \in \mathcal{E}(q)$, where $\mathcal{E}(q)$ is given by (2.1). We have $d = \varphi(q)/r$, since d is the order of the group $(\mathbb{Z}/q\mathbb{Z})^*/_{\mathcal{E}(q)}$. The discrete logarithms of the bad classes are $0, d, 2d, \ldots, (r-1)d$. The set $\mathcal{E}'(q) \cup \mathcal{E}(q)$ is equal to the union of the solutions of the congruences

$$x^2 \equiv g^{ad} \pmod{q} \tag{2.3}$$

for $0 \le a \le r-1$. By the change of variable $x = g^t$, (2.3) is equivalent to

$$2t \equiv ad \pmod{\varphi(q)}. \tag{2.4}$$

Let us assume first that d is odd so that r is even. If a is odd, the congruence (2.4) has no solution while, if a is even, say $a = 2b$, the solutions of (2.4) are $t \equiv bd \pmod{\varphi(q)/2}$ i.e.

$$t \equiv bd \pmod{\varphi(q)} \quad \text{or} \quad t \equiv bd + (r/2)d \pmod{\varphi(q)},$$

which implies

$$\mathcal{E}'(q) \cup \mathcal{E}(q) = \{g^0, g^d, \ldots, g^{(r-1)d}\} = \mathcal{E}(q)$$

and $\mathcal{E}'(q) = \emptyset$.

Let us assume now that d is even. The congruence (2.4) is equivalent to

$$t \equiv ad/2 \pmod{\varphi(q)/2}$$

which implies $\mathcal{E}'(q) \cup \mathcal{E}(q) = \{g^{\alpha d/2}, 0 \le \alpha \le 2r-1\}$ yielding

$$\mathcal{E}'(q) = \{g^{\frac{d}{2}}, g^{3\frac{d}{2}}, \ldots, g^{(2r-1)\frac{d}{2}}\} = \mathcal{C}_b$$

(with $b = (g^{\frac{d}{2}})$), which is coherent by Lemma 2.2.

If $\omega(q) \ge 2$, then, by Lemma 2.1, $\mathcal{E}'(q) \neq \emptyset$. Let $b \in \mathcal{E}'(q)$; by Lemma 2.2, the set $\mathcal{C}_b$ is a coherent set of r elements. □

Let us set

$$c(q) = \begin{cases} \dfrac{3}{2} & \text{if } \mathcal{E}'(q) \neq \emptyset \\ 1 & \text{if } \mathcal{E}'(q) = \emptyset. \end{cases} \tag{2.5}$$

We shall prove

Theorem 2.1. *Let $P \in \mathbb{F}_2[z]$ with $P(0) = 1$, q be the odd integer defined by (1.4) and r be the order of 2 modulo q. We denote by $\mathcal{A}(P)$ the set obtained from (1.1) and by $A(P, x)$ its counting function. When x tends to infinity, we have*

$$A(P, x) \ll_q \frac{x}{(\log x)^{c(q)\frac{r}{\varphi(q)}}}, \tag{2.6}$$

where $c(q)$ is given by (2.5).

When P is irreducible, q is prime and $r = \frac{q-1}{2}$, the upper bound (2.6) is best possible; indeed in this case, from [1], we have $A(P, x) \asymp \frac{x}{(\log x)^{3/4}}$. As $\varphi(q)/r = 2$, Lemma 2.3 implies $\mathcal{E}'(q) \neq \emptyset$ so that $c = 3/2$ and in (2.6), the exponent of $\log x$ is 3/4. Moreover, formula (1.12) gives the optimality of (2.6) for some prime ($q = 31$) satisfying $r = \frac{q-1}{6}$.

Theorem 2.2. *Let $P \in \mathbb{F}_2[z]$ be such that $P(0) = 1$ and $P = P_1 P_2 \cdots P_j$, where the P_i's are irreducible polynomials in $\mathbb{F}_2[z]$. For $1 \leq i \leq j$, we denote by q_i the order of P_i, by r_i the order of 2 modulo q_i and we set $c = \min_{1 \leq i \leq j} c(q_i) r_i/\varphi(q_i)$, where $c(q_i)$ is given by (2.5). When x tends to infinity, we have*

$$A(P, x) \ll \frac{x}{(\log x)^c} \cdot \tag{2.7}$$

where the symbol $\ll$ depends on the q_i's, $1 \leq i \leq j$.

Let $\mathcal{C}$ be a coherent set of semi-bad classes modulo q. Let us associate to $\mathcal{C}$ the set of primes $\mathcal{S}$ defined by

$$p \in \mathcal{S} \iff p \bmod q \in \mathcal{C}. \tag{2.8}$$

We define $\omega_{\mathcal{S}}$ as the additive arithmetic function

$$\omega_{\mathcal{S}}(n) = \sum_{p \mid n,\ p \in \mathcal{S}} 1. \tag{2.9}$$

Lemma 2.4. *Let m be an odd positive integer, not divisible by any bad prime. If $\omega_{\mathcal{S}}(m) = k + 2 \geq 2$ then $2^h m \notin \mathcal{A}(P)$ for all h, $0 \leq h \leq k$. In other words, if $2^h m \in \mathcal{A}(P)$, then $h \geq \omega_{\mathcal{S}}(m) - 1$ holds.*

PROOF. Let us write $\overline{m} = m'm"$, with $m' = \prod_{p|\overline{m}, p\in\mathcal{S}} p$ and $m" = \prod_{p|\overline{m}, p\notin\mathcal{S}} p$. From (1.10), if $n = 2^k m$ then

$$mS_{\mathcal{A}}(m,k) = \sum_{d|\overline{m}} \mu(d)\sigma\left(\mathcal{A}, \frac{n}{d}\right) = \sum_{d'|m'} \sum_{d"|m"} \mu(d')\mu(d")\sigma\left(\mathcal{A}, \frac{n}{d'd"}\right). \qquad (2.10)$$

Let us write $d' = p_{i_1} \cdots p_{i_j}$ and take some $p_{\mathcal{S}}$ from $\mathcal{S}$. If j is even then $\mu(d') = 1$ and, from the definition of a coherent set, $d' \equiv 2^t \pmod{q}$ for some t (depending on d'), $0 \le t \le r-1$. Whereas, if j is odd then $\mu(d') = -1$ and $d' \equiv 2^{t'} p_{\mathcal{S}}^{-1} \pmod{q}$ for some t' (depending on d'), $0 \le t' \le r-1$. From (1.7), we obtain

$$\mu(d')\sigma\left(\mathcal{A}, \frac{n}{d'd"}\right) \equiv \sigma\left(\mathcal{A}, \frac{n}{d"}\right) \pmod{2^{k+1}} \qquad \text{if } j \text{ is even}, \qquad (2.11)$$

$$\mu(d')\sigma\left(\mathcal{A}, \frac{n}{d'd"}\right) \equiv -\sigma\left(\mathcal{A}, \frac{np_{\mathcal{S}}}{d"}\right) \pmod{2^{k+1}} \qquad \text{if } j \text{ is odd}. \qquad (2.12)$$

Since $\alpha = \omega_{\mathcal{S}}(\overline{m}) = k+2 > 0$, the number of d' with odd j is equal to that with even j and is given by

$$1 + \binom{\alpha}{2} + \binom{\alpha}{4} + \cdots = \binom{\alpha}{1} + \binom{\alpha}{3} + \cdots = 2^{\alpha-1}.$$

From (2.10), we obtain

$$mS_{\mathcal{A}}(m,k) \equiv 2^{\alpha-1} \sum_{d"|m"} \mu(d")\left(\sigma\left(\mathcal{A}, \frac{n}{d"}\right) - \sigma\left(\mathcal{A}, \frac{np_{\mathcal{S}}}{d"}\right)\right) \pmod{2^{k+1}}, \quad (2.13)$$

which, as $\alpha = \omega_{\mathcal{S}}(m) = k+2$, gives $S_{\mathcal{A}}(m,k) \equiv 0 \pmod{2^{k+1}}$, so that from (1.8),

$$\chi(\mathcal{A}, m) = \chi(\mathcal{A}, 2m) = \cdots = \chi(\mathcal{A}, 2^k m) = 0. \qquad (2.14)$$

□

Let us assume that $\mathcal{E}'(q) \ne \emptyset$ so that there exists a coherent set $\mathcal{C}$ with r semi-bad classes modulo q; we associate to $\mathcal{C}$ the set of primes $\mathcal{S}$ defined by (2.8) and we denote by $\mathcal{Q} = \mathcal{Q}(q)$ and $\mathcal{N} = \mathcal{N}(q)$ the sets

$$\mathcal{Q} = \{p \text{ prime}, \ p \mid q\} \quad \text{and} \quad \mathcal{N} = \{p \text{ prime}, \ p \notin \mathcal{B} \cup \mathcal{S} \text{ and } \gcd(p, 2q) = 1\},$$

so that the whole set of primes is equal to $\mathcal{B} \cup \mathcal{S} \cup \mathcal{N} \cup \mathcal{Q} \cup \{2\}$. For $n \ge 1$, let us define the multiplicative arithmetic function

$$\delta(n) = \begin{cases} 1 & \text{if } p \mid n \Rightarrow p \notin \mathcal{B} \quad (\text{i.e. } p \in \mathcal{S} \cup \mathcal{N} \cup \mathcal{Q} \cup \{2\}) \\ 0 & \text{otherwise.} \end{cases}$$

and for $x > 1$,

$$V(x) = V_q(x) = \sum_{n \ge 1, \ n2^{\omega_{\mathcal{S}}(n)} \le x} \delta(n). \qquad (2.15)$$

Lemma 2.5. *Under the above notation, we have*

$$V(x) = V_q(x) = \mathcal{O}_q\left(\frac{x}{(\log x)^{c(q)\frac{r}{\varphi(q)}}}\right), \tag{2.16}$$

where $c(q)$ is given by (2.5).

Proof. To prove (2.16), one should consider, for complex s with $\mathcal{R}(s) > 1$, the series

$$F(s) = \sum_{n\geq 1} \frac{\delta(n)}{(n2^{\omega_S(n)})^s}. \tag{2.17}$$

This Dirichlet series has an Euler's product given by

$$F(s) = \prod_{p\in\mathcal{N}\cup\mathcal{Q}\cup\{2\}} \left(1-\frac{1}{p^s}\right)^{-1} \prod_{p\in\mathcal{S}} \left(1+\frac{1}{2^s(p^s-1)}\right), \tag{2.18}$$

which can be written as

$$F(s) = H(s) \prod_{p\in\mathcal{N}} \left(1-\frac{1}{p^s}\right)^{-1} \prod_{p\in\mathcal{S}} \left(1-\frac{1}{p^s}\right)^{-\frac{1}{2^s}}, \tag{2.19}$$

where

$$H(s) = \prod_{p\in\mathcal{Q}\cup\{2\}} \left(1-\frac{1}{p^s}\right)^{-1} \prod_{p\in\mathcal{S}} \left(1+\frac{1}{2^s(p^s-1)}\right)\left(1-\frac{1}{p^s}\right)^{\frac{1}{2^s}}. \tag{2.20}$$

By applying Selberg–Delange's formula (cf. [8], Théorème 1 and [9], Lemma 4.5), we obtain some constant c_4 such that

$$V(x) = c_4 \frac{x}{(\log x)^{c(q)\frac{r}{\varphi(q)}}} + \mathcal{O}_q\left(\frac{x\log\log x}{\log x}\right). \tag{2.21}$$

The constant c_4 is somewhat complicated, it is given by

$$c_4 = \frac{CH(1)}{\Gamma(1-c(q)\frac{r}{\varphi(q)})}, \tag{2.22}$$

where Γ is the gamma function,

$$H(1) = \frac{2q}{\varphi(q)} \prod_{p\in\mathcal{S}} \left(1+\frac{1}{2(p-1)}\right)\left(1-\frac{1}{p}\right)^{\frac{1}{2}} \tag{2.23}$$

and

$$C = \prod_{p\in\mathcal{N}} \left(1-\frac{1}{p}\right)^{-1} \prod_{p\in\mathcal{S}} \left(1-\frac{1}{p}\right)^{\frac{-1}{2}} \prod_{p} \left(1-\frac{1}{p}\right)^{1-c(q)\frac{r}{\varphi(q)}},$$

where in the third product, p runs over all primes. □

3. Proof of the results

PROOF OF THEOREM 2.1. If $r = \varphi(q)$ then 2 is a generator of $(\mathbb{Z}/q\mathbb{Z})^*$, all primes are bad but 2 and the prime factors of q; hence by Theorem 2 of [5], $A(P,x) = \mathcal{O}((\log x)^\kappa)$ for some constant κ, so that we may remove the case $r = \varphi(q)$.

If $\mathcal{E}'(q) = \emptyset$, from (2.5), $c = 1$ holds and (2.6) follows from (1.16).

We now assume $\mathcal{E}'(q) \neq \emptyset$, so that, from Lemma 2.2, there exists a coherent set $\mathcal{C}$ satisfying $|\mathcal{C}| = r$. We define the set of primes $\mathcal{S}$ by (2.8). Let us write $V(x)$ defined in (2.15) as

$$V(x) = V'(x) + V"(x), \tag{3.1}$$

with

$$V'(x) = \sum_{n\geq 1,\ n2^{\omega_{\mathcal{S}}(n)}\leq x,\ \omega_{\mathcal{S}}(n)=0} \delta(n) \quad \text{and} \quad V"(x) = \sum_{n\geq 1,\ n2^{\omega_{\mathcal{S}}(n)}\leq x,\ \omega_{\mathcal{S}}(n)\geq 1} \delta(n).$$

Similarly, we write $A(P,x) = \sum_{a\in\mathcal{A}(P),\ a\leq x} 1 = A' + A"$, with

$$A' = \sum_{a\in\mathcal{A}(P),\ a\leq x,\ \omega_{\mathcal{S}}(a)=0} 1 \quad \text{and} \quad A" = \sum_{a\in\mathcal{A}(P),\ a\leq x,\ \omega_{\mathcal{S}}(a)\geq 1} 1.$$

An element a of $\mathcal{A}(P)$ counted in A' is free of bad and semi-bad primes, so that

$$A' \leq V'(x) \leq V'(2x). \tag{3.2}$$

By Lemma 2.4, an element a of $\mathcal{A}(P)$ counted in $A"$ is of the form $n2^{\omega_{\mathcal{S}}(n)-1}$ with $\omega_{\mathcal{S}}(n) = \omega_{\mathcal{S}}(a) \geq 1$; hence

$$A" \leq V"(2x). \tag{3.3}$$

Therefore, from (3.1)–(3.3), we get

$$A(P,x) = A' + A" \leq V'(2x) + V"(2x) = V(2x)$$

and (2.6) follows from Lemma 2.5. □

PROOF OF THEOREM 2.2. Just use Theorem 2.1 and (1.13). □

ACKNOWLEDGEMENTS. It is a great pleasure for us to thank ANDRÁS SÁRKÖZY for initiating the study of the sets $\mathcal{A}(P)$ and for all the mathematics that we have learnt from him.

References

[1] N. BACCAR and F. BEN SAÏD, On sets such that the partition function is even from a certain point on, *Int. J. Number Theory* 5, no. 3 (2009), 1–22.

[2] N. BACCAR, F. BEN SAÏD and A. ZEKRAOUI, On the divisor function of sets with even partition functions, *Acta Math. Hungar.* **112**(1–2) (2006), 25–37.

[3] F. BEN SAÏD, On a conjecture of Nicolas–Sárközy about partitions, *J. Number Theory* **95** (2002), 209–226.

[4] F. BEN SAÏD, On some sets with even valued partition function, *Ramanujan J.* **9** (2005), 63–75.

[5] F. BEN SAÏD, H. LAHOUAR and J.-L. NICOLAS, On the counting function of the sets of parts $\mathcal{A}$ such that the partition function $p(\mathcal{A}, n)$ takes even values for n large enough, *Discrete Math.* **306** (2006), 1115-1125.

[6] F. BEN SAÏD and J.-L. NICOLAS, Sets of parts such that the partition function is even, *Acta Arith.* **106** (2003), 183–196.

[7] F. BEN SAÏD and J.-L. NICOLAS, Even partition functions, Séminaire Lotharingien de Combinatoire (`http//www.mat.univie.ac.at/~slc/`), Vol. 46, 2002, B 46i.

[8] F. BEN SAÏD and J.-L. NICOLAS, Sur une application de la formule de Selberg–Delange, *Colloq. Math.* **98**, no. 2 (2003), 223–247.

[9] F. BEN SAÏD, J.-L. NICOLAS and A. ZEKRAOUI, On the parity of generalised partition function III, *J. Théor. Nombres Bordeaux* **22** (2010), 51–78.

[10] LI-XIA DAI and YONG-GAO CHEN, On the parity of the partition function, *J. Number Theory* **122** (2007), 283–289.

[11] H. LAHOUAR, Fonctions de partitions à parité périodique, *European J. of Combin.* **24** (2003), 1089–1096.

[12] R. LIDL and H. NIEDERREITER, Introduction to finite fields and their applications, *Cambridge University Press*, 1994, revised edition.

[13] J.-L. NICOLAS, I. Z. RUZSA and A. SÁRKÖZY, On the parity of additive representation functions, *J. Number Theory* **73** (1998), 292–317.

[14] J.-L. NICOLAS and A. SÁRKÖZY, On the parity of partition functions, *Illinois J. Math.* **39** (1995), 586–597.

[15] J.-L. NICOLAS and A. SÁRKÖZY, On the parity of generalised partition functions, in: Number theory for the millenium, III (Urbana, Il, 2000), 55-72, *A. K. Peters, Natick, MA*, 2002.

FETHI BEN SAÏD
UNIVERSITÉ DE MONASTIR
FACULTÉ DES SCIENCES DE MONASTIR
AVENUE DE L'ENVIRONNEMENT
5000 MONASTIR
TUNISIE

E-mail: Fethi.BenSaid@fsm.rnu.tn

JEAN-LOUIS NICOLAS
UNIVERSITÉ DE LYON
UNIVERSITÉ LYON 1, CNRS
INSTITUT CAMILE JORDAN, MATHÉMATIQUES
BATIMENT DOYEN JEAN BRACONNIER
UNIVERSITÉ CLAUDE BERNARD
21 AVENUE CLAUDE BERNARD
F-69622 VILLEURBANNE CEDEX
FRANCE

E-mail: jlnicola@in2p3.fr

(Received February 3, 2011; revised August 16, 2011)